Exhibit A

AFFIDAVIT OF SPECIAL AGENT BRYCE FERRARA IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Special Agent Bryce Ferrara, state:

INTRODUCTION AND AGENT BACKGROUND

1. I am a federal law enforcement officer within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request arrest warrants and search warrants. I am currently employed as a Special Agent with the Federal Bureau of Investigation ("FBI") and have been so employed since January 2019. I am currently assigned to the FBI Boston Violent Crimes Task Force ("VCTF"), which is comprised of personnel from the FBI and Massachusetts State Police, as well as from the Boston, Braintree, Malden, Saugus, Somerville, and Dedham Police Departments.

2. As a Special Agent with the VCTF, I have regularly responded to incidents involving violent encounters. I have also received specialized training regarding investigative techniques, evidence collection, and evidence preservation. My responsibilities include the investigation of possible violations of federal law, including investigation of violent crimes like armed robberies, bank robberies, and threats/extortion. In the course of my career, my investigations have included the use of various surveillance techniques and the execution of various search, seizure, and arrest warrants.

PURPOSE OF AFFIDAVIT

3. The VCTF and the Boston Police Department are conducting a criminal investigation of Trevor LUCAS ("LUCAS") in connection with possible violations of, among other statutes, 21 U.S.C. § 841(a)(1), possession of a controlled substance with intent to distribute or dispense, 21 U.S.C. § 844(a), possession of a controlled substance, and 18 U.S.C. §

1343 (wire fraud).

4. This affidavit is being submitted in support of an application for a warrant to search the premises located at 143 Fulton Street, First and Third Floors, in Boston, Massachusetts ("RESIDENCE"), as further described in Attachment A, because there is probable cause to believe that it contains evidence, fruits, and instrumentalities of violations of 21 U.S.C. § 841(a)(1), 21 U.S.C. § 844(a), and 18 U.S.C. § 1343 (the "TARGET OFFENSES"), as described in Attachment B.

5. The facts in this affidavit come from my personal observations and review of records, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is probable cause for the requested search warrant and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE TO BELIEVE THAT A FEDERAL CRIME WAS COMMITTED

6. I am aware that the Drug Enforcement Administration ("DEA") has published information regarding Gamma-hydroxybutyric acid ("GHB") and that GHB is a Schedule I depressant, per the Controlled Substances Act. The GHB-containing pharmaceutical product, Xyrem, is controlled as a Schedule III drug. DEA publications indicate that GHB abuse became popular among teens and young adults at dance clubs and "raves" in the 1990s and gained notoriety as a date rape drug. Possession of a controlled substance with the intent to distribute or dispense is a violation of Title 21, United States Code, Section 841(a)(1). Simple possession of a controlled substance without a valid prescription or other authority is a violation of Title 21, United States Code, Section 844(a).

7. In February 2020, an anonymous tip was sent to CrimeStoppers, a service offered by the Boston Police Department that allows people to provide anonymous information about

criminal activity. The anonymous tip related to statements and actions of Trevor LUCAS.

8. In 2009, LUCAS was arrested and charged with several federal crimes arising out of an attempted kidnapping in Wisconsin. He ultimately pleaded guilty to one of the charges, intentionally brandishing a gun during and in relation to a crime of violence under 18 U.S.C. § 924(c), and was sentenced to 210 months in prison.

9. The anonymous tip submitted to CrimeStoppers in February 2020 stated as follows:

> I MET THIS GUY TREVOR LUCAS , WHITE MALE EARLY 30'S , BALD W/BLUE EYES , 5'11" , 180LBS , DOB xx/xx/88 , PHONE # xxx-xxx-9991. I BELIEVE HE LIVES AT 143 FULTON ST , 3 RD ,FLR WITH A PATRIOTS STICKER ON THE DOOR. HE WAS RECENTLY DUMPED BY HIS BOYFRIEND . I'VE BEEN VISITING AS A FRIEND . I BECAME NERVOUS WHEN HE STATED HE IS A FORMER CONVICT , AND HE WAS ASKING A LOT OF QUESTIONS ABOUT HOW TO KILL SOMEONE WITHOUT GETTING CAUGHT. I TRIED TO PLAY IT COOL BECAUSE I WAS IN HIS HOUSE AND I FELT IN DANGER IF I TRIED TO LEAVE . I WORK IN A LAB AND HE WAS ASKING IF A LAB WORKER COULD GET THEIR HANDS ON ANYTHING THAT COULD PARALYZE OR KILL A PERSON IF THE RIGHT PRICE WAS GIVEN . I SAID I WOULD THINK ABOUT IT . I'M CONCERNED FOR THE SAFETY OF THESE PEOPLE. HE IS FINALIZING THE PURCHASE OF A HOUSE FOR HIS EX BOYFRIEND IN CHICOPEE MASS.. PLEASE, I DIDN'T REACH OUT RIGHT AWAY FOR REAR OF MY SAFETY, HE'S BEEN CALLING AND TEXTING ME TO ASK TO MEET AGAIN , I'M SCARED . HE TOLD ME HE GOTTEN APPROVAL FROM HIS FEDERAL PROBATION OFFICER BUT NOT HIS STATE PO TO GO TO A CAR RACE IN FLORIDA WITH HIS EX BOYFRIEND. PLEASE I'M CONCERNED FOR MY LIFE. NO FURTHER INFO . TIP # 200208.

10. Boston Police received the above information from CrimeStoppers, reviewed the tip, and attempted to contact the anonymous individual who had submitted the tip ("INDIVIDUAL"). In late February 2020, Boston Police contacted the FBI for assistance in the investigation. In early March 2020, Boston Police contacted INDIVIDUAL, who agreed to meet for an interview with the Boston Police and FBI.

Information Reported by INDIVIDUAL

11. During the initial interview, INDIVIDUAL reported that LUCAS spoke about acquiring chemicals to kill or paralyze an unknown person. LUCAS also asked INDIVIDUAL if he could procure a fake identification so that LUCAS could leave the Commonwealth of Massachusetts without the knowledge of his probation officer.[1] INDIVIDUAL ascertained that LUCAS was jealous of an ex-partner and the ex-partner's relationships with other people.

12. Based on my training and experience, my work during the course of this investigation, and through conversations with other law enforcement agents, I believe INDIVIDUAL to be credible, and I understand that certain information provided by INDIVIDUAL has been corroborated by the FBI and found to be accurate.

13. In early February 2020, LUCAS gave INDIVIDUAL approximately $240, passport-style photographs of himself, and a signature card with the name "James McCalester" written or signed by hand. LUCAS requested that INDIVIDUAL obtain a fake identification for him using the information and materials provided. INDIVIDUAL subsequently provided the FBI with the passport photos and signature card.

14. On March 5, 2020, INDIVIDUAL contacted Boston Police by phone regarding a meeting that took place earlier the same day at RESIDENCE.[2] During their meeting, LUCAS told INDIVIDUAL that he has accessed the "dark web" to procure various items, including a "whole cocktail" of drugs. INDIVIDUAL observed a "whole cocktail" of drugs located in apartment "0", on the first floor of RESIDENCE. While at RESIDENCE, INDIVIDUAL

[1] LUCAS is currently on federal and state supervised release arising out of the above-mentioned federal conviction.

[2] FBI surveillance in the vicinity of LUCAS's residence on March 5, 2020 confirmed that INDIVIDUAL did, in fact, visit LUCAS at RESIDENCE that day.

observed the laptop that LUCAS purportedly uses to access the dark web; that laptop is of an unknown brand and bears an "Eagle Eye" logo.

15. LUCAS showed INDIVIDUAL quantities of GHB in liquid form packaged as a sports energy drink, which LUCAS told INDIVIDUAL he had purchased on the "dark web." LUCAS informed INDIVIDUAL that he had researched GHB to determine what dose of the drug would be enough to incapacitate a person.

16. Based on my training and experience, I understand that individuals who obtain drugs via the dark web generally lack prescriptions or other authority for such drugs, and that a primary reason that individuals use the dark web to obtain drugs is that no proof of prescriptions or other authority is required.

Interactions Between LUCAS and FBI Undercover Employee

17. In the course of our investigation, an FBI Undercover Employee ("UCE") was introduced to LUCAS for the purpose of further investigating LUCAS's plans. LUCAS and UCE have been in contact via email and phone, as well as through several in-person meetings, since March 24, 2020.

18. In April 2020, LUCAS mailed UCE payment in the form of a U.S. Postal Service money order for the purpose of acquiring a fake New Hampshire driver's license. U.S. Postal Service inspectors determined that the money order was purchased at the Hanover Street Post Office in Boston, Massachusetts. The money order was entered into FBI evidence.

19. On May 12, 2020, LUCAS and UCE met in Massachusetts at a pre-determined meeting location. UCE provided LUCAS with an FBI-manufactured New Hampshire driver's license. During their meeting, LUCAS asked UCE about acquiring U.S. Postal Service money orders for a scheme he had devised to defraud individuals yet unknown and stated that also he

plans to conduct an auto registration scam against individuals yet unknown. Toward the end of their meeting, LUCAS and UCE discussed the possibility of LUCAS purchasing a firearm from UCE. LUCAS asked UCE what other products UCE could provide to LUCAS, and LUCAS asked about the potential price of a firearm.

20. On May 30, 2020, LUCAS and UCE met at RESIDENCE and discussed, among other things, the scheme in which LUCAS was planning to utilize fraudulent U.S. Postal Service money orders. UCE showed LUCAS templates of fraudulent money orders. LUCAS and UCE discussed the possibility of UCE obtaining a stun gun and a firearm for LUCAS to purchase.

21. During the same meeting, LUCAS told UCE that his had father had purchased RESIDENCE in 1969 for $5,000. LUCAS told UCE that he does not have to pay rent because his father still owns the building. LUCAS showed UCE the first-floor unit that he has been using as a workshop and explained that he is adding a wall to the first-floor apartment to convert the unit into two separate apartments. LUCAS told UCE that he is performing the renovations on the first-floor unit himself, but for the electrical work.

22. Records maintained by the Massachusetts Registry of Motor Vehicles, LUCAS resides at RESIDENCE. Based on surveillance and witness statements, I understand that LUCAS lives in the sole unit on the third floor of the building and that LUCAS has regular access to and has utilized the vacant unit on the first floor as a workshop and for the purpose of personally renovating the first floor of the building.[3]

[3] On July 25, 2020, Special Agent Bryce Ferrara drove past RESIDENCE and observed an Apartments.com "Rent" sign in the window of an apartment located on the first-floor of the RESIDENCE.

LUCAS's Requests for Firearms and Cyanide

23. On June 14, 2020, LUCAS and UCE engaged in a recorded telephone call, largely in regard to items that UCE could obtain for LUCAS. LUCAS requested that UCE provide him with three firearms: a Glock pistol, a 9mm Beretta pistol, and a .357 Magnum handgun. LUCAS requested that the Glock and the Beretta be black or blue and that the .357 Magnum be steel. UCE indicated that he would be willing to sell LUCAS all three firearms for $3,500. LUCAS inquired about the fraudulent money orders that he believed UCE was making or obtaining for LUCAS. They discussed the provision of ten initial money orders for LUCAS in exchange for $1,000. LUCAS and UCE discussed printers and templates relating to the money order scam. Just before the call ended, LUCAS asked that UCE also provide LUCAS with something to "fill up" the items LUCAS had agreed to purchase from UCE. I believe that the request for something to "fill up" the purchased items was a reference to ammunition for the firearms.

24. From June 13, 2020 to June 14, 2020, UCE and an individual presumed to be LUCAS corresponded using a pre-designated email account and the "Drafts" folder within that account. The correspondence included photographs of items for potential procurement by LUCAS based on a prior conversation, including photos of one stun gun and one firearm.

25. On June 25, 2020, LUCAS and UCE engaged in a recorded Facetime audio call.[4] UCE informed LUCAS that the fraudulent money orders, stun gun and three firearms that LUCAS had requested were ready for delivery. LUCAS and UCE also discussed the timing for when they could meet to complete the transaction and a final price of $4,500 for the stun gun,

[4] Along with other telephonic and/or electronic communications between LUCAS and UCE, I understand that this communication was transmitted by means of wire and that the device(s) on which the communications took place constitutes a means, facility, and/or instrumentality of interstate commerce.

three firearms, and the fraudulent money orders.

26. On July 20, 2020, LUCAS and UCE engaged in a recorded telephone call. LUCAS and UCE discussed details regarding the fraudulent money orders and stun gun that LUCAS was planning to procure from UCE. Regarding firearms, LUCAS informed UCE that he was waiting to hear from one of his "buddies" driving from Virginia, potentially with firearms. LUCAS explained that he wanted to see what his "buddy" was doing prior to committing to a purchase of firearm(s) from UCE. LUCAS and UCE discussed the price for one potential handgun.

27. During the same call, LUCAS asked UCE, "[W]hat do you … do you have anything relating to, um, cyanide, or any type of … strong … knock you out type of stuff?" The UCE responded, "Uh, just knock you out?" LUCAS responded, "I mean, completely. Like, for good knock out." LUCAS added, "I got … I got stuff to knock you out for a few hours. I already have that." LUCAS requested that UCE provide a price before making a purchase for him. LUCAS and UCE concluded the conversation with a plan to talk again on July 23, 2020.

THE PREMISES CONTAINS EVIDENCE, FRUITS, AND INSTRUMENTALITIES

28. I observed the residential structure located at 143 Fulton Street in Boston, Massachusetts to be a red brick, multi-tier, multi-unit building abutted by other buildings of similar structure and color. The unit to be searched is the sole unit located on the third floor of the building and the unit on the first floor of the building. The premises to be searched are more fully described in Attachment A to the search warrant application.

29. I also have probable cause to believe that the premises to be searched contains fruits, evidence, and instrumentalities of violations of the TARGET OFFENSES, as described in Attachment B.

30. I believe that evidence of criminal activity is likely to be found at RESIDENCE because, among other things, (1) LUCAS informed INDIVIDUAL that he has accessed the "dark web" on his laptop computer, located in RESIDENCE, to procure GHB and/or other drugs; (2) LUCAS showed INDIVIDUAL what he described as a "whole cocktail of drugs" in the first-floor unit of RESIDENCE; (3) LUCAS showed INDIVIDUAL quantities of GHB in liquid form packaged as a sports energy drink at RESIDENCE; (4) LUCAS told UCE that he is currently in possession of enough "stuff," in a conversation about cyanide and/or other drugs, that he can "knock out" someone; (5) LUCAS has been attempting to procure chemicals and/or drugs in lethal doses since at least February 2020 and as recently as July 20, 2020, when he asked UCE if UCE could procure on his behalf a lethal dose of cyanide; (6) based on my training and experience, individuals who possess GHB and other controlled substances frequently store their drugs at their primary place of residence; (7) using a computer, smartphone, or other device connected to the internet, LUCAS exchanged electronic messages with UCE about procuring, among other things, fraudulent money orders as part of a scheme to defraud persons yet unknown; and (7) my investigation has confirmed that LUCAS resides at RESIDENCE.

31. Based on my training and experience, as well as through communications with other members of law enforcement, I understand that while individuals sometimes use smartphones for email and internet searches, they also frequently use desktop, laptop, or tablet computers for such purposes, and often keep such devices where they reside.

SEIZURE OF COMPUTER EQUIPMENT AND DATA

32. From my training, experience, and information provided to me by other agents, I am aware that individuals frequently use computers to create and store records of their actions by

communicating about them through email, instant messages, and updates to online social-networking websites; drafting letters; keeping their calendars; arranging for travel; storing pictures; researching topics of interest; buying and selling items online; and accessing their bank, financial, investment, utility, and other accounts online.

33. Based on my training, experience, and information provided by other law enforcement officers, I know that many cell phones (which are included in Attachment B's definition of "hardware") can now function essentially as small computers. Phones have capabilities that include serving as a wireless telephone to make audio calls, digital camera, portable media player, GPS navigation device, sending and receiving text messages and emails, and storing a range and amount of electronic data. Examining data stored on devices of this type can uncover, among other things, evidence of communications and evidence of communications and evidence that reveals or suggests who possessed or used the device.

34. Based on my knowledge, training, experience, and information provided to me by other agents, I know that computer files or remnants of such files can be recovered months or years after they have been written, downloaded, saved, deleted, or viewed locally or over the internet. This is true because:

a. Electronic files that have been downloaded to a storage medium can be stored for years at little or no cost. Furthermore, when users replace their computers, they can easily transfer the data from their old computer to their new computer.

b. Even after files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a

computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data, which might not occur for long periods of time. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media – in particular, computers' internal hard drives – contain electronic evidence of how the computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. It is technically possible to delete this information, but computer users typically do not erase or delete this evidence because special software is typically required for that task.

d. Similarly, files that have been viewed over the internet are sometimes automatically downloaded into a temporary internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed internet pages or if a user takes steps to delete them.

e. Data on a storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers,

email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

f. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used.

For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such

evidence in an effort to conceal it from law enforcement).

g. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

h. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

i. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

35. Based on my knowledge and training and the experience of other agents with whom I have spoken, I am aware that in order to completely and accurately retrieve data maintained in computer hardware, computer software or storage media, to ensure the accuracy

and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that computer hardware, computer software, and storage media ("computer equipment") be seized and subsequently processed by a computer specialist in a laboratory setting rather than in the location where it is seized. This is true because of:

a. The volume of evidence – storage media such as hard disks, flash drives, CDs, and DVDs can store the equivalent of thousands or, in some instances, millions of pages of information. Additionally, a user may seek to conceal evidence by storing it in random order or with deceptive file names. Searching authorities may need to examine all the stored data to determine which particular files are evidence, fruits, or instrumentalities of criminal activity. This process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this analysis on-site.

b. Technical requirements – analyzing computer hardware, computer software or storage media for criminal evidence is a highly technical process requiring expertise and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know, before the search, which expert possesses sufficient specialized skill to best analyze the system and its data. Furthermore, data analysis protocols are exacting procedures, designed to protect the integrity of the evidence and to recover even "hidden" deleted, compressed, or encrypted files. Many commercial computer software

programs also save data in unique formats that are not conducive to standard data searches. Additionally, computer evidence is extremely vulnerable to tampering or destruction, both from external sources and destructive code imbedded in the system as a "booby trap"

Consequently, law enforcement agents may either copy the data at the premises to be searched or seize the computer equipment for subsequent processing elsewhere.

36. The premises may contain computer equipment whose use in the crime or storage of the things described in this warrant is impractical to determine at the scene. Computer equipment and data can be disguised, mislabeled, or used without the owner's knowledge. In addition, technical, time, safety, or other constraints can prevent definitive determination of their ownership at the premises during the execution of this warrant. If the things described in Attachment B are of the type that might be found on any of the computer equipment, this application seeks permission to search and seize it onsite or off-site in order to determine their true use or contents, regardless of how the contents or ownership appear or are described by people at the scene of the search.

37. The law enforcement agents will endeavor to search and seize only the computer equipment which, upon reasonable inspection and/or investigation conducted during the execution of the search, reasonably appear to contain the evidence in Attachment B. If however, the law enforcement agents cannot make a determination as to use or ownership regarding any particular device, the law enforcement agents will seize and search that device pursuant to the probable cause established herein.

38. This warrant authorizes a review of electronic storage media seized, electronically stored information, communications, other records and information seized, copied or disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, FBI may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review

CONCLUSION

39. Based on the information described above, I have probable cause to believe that that Trevor LUCAS, DOB xx/xx/1988, has violated 21 U.S.C. § 841(a)(1) (possession of a controlled substance with intent to distribute or dispense), 21 U.S.C. § 844(a) (possession of a controlled substance), and 18 U.S.C. § 1343 (wire fraud).

(continued on next page)

40. Based on the information described above, I also have probable cause to believe that evidence, fruits, and instrumentalities of this crime, as described in Attachment B, are contained within the premises described in Attachment A.

Sworn to under the pains and penalties of perjury,

/s/ Bryce Ferrare DLC
Bryce Ferrara, Special Agent
Federal Bureau of Investigation

Subscribed and sworn to via telephone in accordance with Fed. R. Crim. P. 4.1 on July 29, 2020.

Hon. Donald L. Cabell
United States Magistrate Judge

ATTACHMENT A

DESCRIPTION OF THE PREMISES TO BE SEARCHED

The premises to be searched are located at 143 Fulton Street, First and Third Floor, Boston, Massachusetts. The building at 143 Fulton Street is a red brick, multi-tier, multi-unit building abutted by other buildings of similar structure and color. The number "143" is clearly labeled on the building, to the left of the front breezeway. The units to be searched are those located on the first and third floors of the building.

ATTACHMENT B

ITEMS TO BE SEIZED

I. All records, in whatever form, and tangible objects that constitute evidence, fruits, or instrumentalities of violations of 21 U.S.C. § 841(a)(1), 21 U.S.C. § 844(a), and 18 U.S.C. § 1343 including:

A. Records and tangible objects pertaining to the following topics:

1. controlled substances, including but not limited to GHB, drug packaging material, and related paraphernalia;
2. any scheme or artifice to defraud involving fraudulent money orders, as well as communications about any such scheme; and
3. communications with any undercover agent(s) of the Federal Bureau of Investigation between March - July 2020, or any records or objects relating to or referencing such communications or such agent(s);

B. For any computer hardware, computer software, mobile phones, or storage media called for by this warrant or that might contain things otherwise called for by this warrant ("the computer equipment"):

1. evidence of who used, owned, or controlled the computer equipment;
2. evidence of the presence or absence of malicious software that would allow others to control the items, and evidence of the presence or absence of security software designed to detect malicious software;

3. evidence of the attachment of other computer hardware or storage media;

4. evidence of counter-forensic programs and associated data that are designed to eliminate data;

5. evidence of when the computer equipment was used;

6. passwords, encryption keys, and other access devices that may be necessary to access the computer equipment;

7. records and tangible objects pertaining to accounts held with companies providing Internet access or remote storage;

C. Records and tangible objects relating to the ownership, occupancy, or use of the premises to be searched (such as utility bills, phone bills, rental or lease agreements, rent payments, mortgage bills and/or payments, photographs, insurance documentation, receipts, and check registers); and

II. All computer hardware, computer software, and storage media. Off-site searching of these items shall be limited to searching for the items described in paragraph I.

DEFINITIONS

For the purpose of this warrant:

A. "Computer equipment" means any computer hardware, computer software, mobile phone, storage media, and data.

B. "Computer hardware" means any electronic device capable of data processing (such as a computer, smartphone, cell/mobile phone, or wireless communication device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable

storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).

C. "Computer software" means any program, program code, information or data stored in any form (such as an operating system, application, utility, communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.

D. "Storage media" means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, or memory card).

E. "Data" means all information stored on storage media of any form in any storage format and for any purpose.

F. "A record" is any communication, representation, information or data. A "record" may be comprised of letters, numbers, pictures, sounds or symbols.

RETURN OF SEIZED COMPUTER EQUIPMENT

If the owner of the seized computer equipment requests that it be returned, the government will attempt to do so, under the terms set forth below. If, after inspecting the seized computer equipment, the government determines that some or all of this equipment does not contain contraband or the passwords, account information, or personally-identifying information of victims, and the original is no longer necessary to retrieve and preserve as evidence, fruits or

instrumentalities of a crime, the equipment will be returned within a reasonable time, if the party seeking return will stipulate to a forensic copy's authenticity (but not necessarily relevancy or admissibility) for evidentiary purposes.

If computer equipment cannot be returned, agents will make available to the computer system's owner, within a reasonable time period after the execution of the warrant, copies of files that do not contain or constitute contraband; passwords, account information, or personally-identifying information of victims; or the fruits or instrumentalities of crime.

For purposes of authentication at trial, the Government is authorized to retain a digital copy of all computer equipment seized pursuant to this warrant for as long as is necessary for authentication purposes.